Claims:

1. An integrated firewall/VPN system, comprising:

at least one wide area network (WAN);

at least one local area network (LAN); and

an integrated firewall/VPN chipset adapted to send and receive data packets between said WAN and said LAN, said chipset comprising a firewall portion and to provide access control between said WAN and said LAN and a VPN portion adapted to provide security functions for data between said LAN and said WAN; said firewall including firewall hardware and software portions wherein at least said firewall hardware portion is adapted to provide iterative functions associated with said access control; said VPN potion including VPN hardware and software portions wherein at least VPN hardware portion is adapted to provide iterative functions associated with said security functions.

2. A system as claimed in claim 1, wherein said chipset further comprises a router adapted to route data between said LAN and said LAN.

3. A system as claimed in claim 1, wherein said firewall hardware portion comprising circuitry to provide static and/or dynamic data packet filtering.

4. A system as claimed in claim 3, wherein said circuitry includes a header match packet filtering circuit to provide pattern matching in selected headers of said data.

5. A system as claimed in claim 1, wherein said chipset further adapted to analyze access control functions based on preselected bytes of said data packets.

6. A system as claimed in claim 5, wherein said preselected bytes comprise the first 144 bytes of said data packet.

7. A system as claimed in claim 1, wherein said VPN security functions comprise,

encryption, decryption, encapsulation, and decapsulation of said data packets.

8. A system as claimed in claim 1, wherein said firewall access control functions comprise user-defined access control protocols.

9. A firewall/VPN integrated circuit (IC), comprising:

a router core adapted to interface between at least one untrusted network and at least one trusted network to send and receive data packets between said untrusted and said trusted networks;

a firewall system adapted to provide access control between said untrusted and said trusted networks, and comprising firewall hardware and software portions wherein at least said firewall hardware portion is adapted to provide iterative functions associated with said access control; and

a VPN engine adapted to provide security functions for data between said untrusted and said trusted networks, and comprising VPN hardware and software wherein at least said VPN hardware portion is adapted to provide iterative functions associated with said security functions.

10. An IC system as claimed in claim 9, wherein said firewall hardware portion comprising circuitry to provide static and/or dynamic data packet filtering.

11. An IC as claimed in claim 10, wherein said circuitry includes a header match packet filtering circuit to provide pattern matching in selected headers of said data.

12. An IC as claimed in claim 9, wherein said firewall system further adapted to analyze access control functions based on preselected bytes of said data packets.

13. An IC as claimed in claim 12, wherein said preselected bytes comprise the first 144 bytes of said data packet.

14. A system as claimed in claim 9, wherein said VPN security functions comprise, encryption, decryption, encapsulation, and decapsulation of said data packets.

15. A system as claimed in claim 9, wherein said firewall access control functions comprise user-defined access control protocols.

16. A method of providing firewall access control functions, comprising the steps of:

defining one or more access control protocols;

receiving a data packet;

selecting a certain number of bytes of said data packet;

processing said selected bytes using said access control protocols.

17. A method as claimed in claim 16, further comprising the steps of:

providing hardware implementation of static and/or dynamic packet data filtering using said access control protocols.